THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA

SMARTMATIC USA CORP., SMARTMATIC INTERNATIONAL HOLDING B.V. and SGO CORPORATION LIMITED, Plaintiffs, v. MICHAEL J. LINDELL and MY PILLOW, INC., Defendants.	Case No. 22-cv-00098-WMW-JFD

DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION TO EXCLUDE EXPERT REPORT AND TESTIMONY OF BENJAMIN COTTON (DKT. 414)

MCSWEENEY, CYNKAR & KACHOUROFF, PLLC

By */s/ Christopher I. Kachouroff*
Christopher I. Kachouroff* (Bar No. 44216)
13649 Office Place, Suite 101
Woodbridge, Virginia 22192
Telephone: (703) 621-3300
chris@mck-lawyers.com

Douglas G. Wardlow (MN Bar #339544)
Jeremiah D. Pilon (MN Bar #392825)
1550 Audubon Rd.
Chaska, MN 55318
Telephone: (952) 826-8658
doug@mypillow.com
jpilon@mypillow.com

ATTORNEY FOR MY PILLOW, INC. AND MICHAEL LINDELL
*Admitted *Pro Hac Vice*

PRELIMINARY STATEMENT

A voting machine, including the L.A. County machine that Smartmatic built to 3rd party specifications, is nothing more than a computer system built with Commercial Off-the-Shelf (COTS) components. The hardware used for voting machines may include things like a motherboard, a hard drive, a chipset, USB ports, a screen, wired ethernet access, wireless or Bluetooth connectivity, an operating system, motherboards, and other standard components. But it may also have specialized software applications that run off a standard operating system. In other words, it is a computer with both internal and external components. Benjamin Cotton is a cyber security expert specializing in forensic examinations of computerized systems.

In terms of educational background, there is no formal education degree for voting machine security any more than there would be for White House computer systems, TSA's specialized checkpoint scanners, or the ECF filing system used by U.S. Courts. After all, a voting machine is a computer system made from commercial off-the-shelf components and there is no formal education in "voting machine technology." In short, Mr. Cotton's credentials speak for themselves.

Mr. Cotton's experience is not purely academia research, although he has taught cybersecurity investigation for decades. *See* Decl. Cotton. He is not being offered to prove that Smartmatic rigged or stole the 2020 election using L.A. County's system. Rather, Mr. Cotton is being offered as a cyber security expert in the area of forensic examination of computer systems and networks. He has examined electronic voting systems which call into question the integrity of post-election audits. *See, e.g.,* Decl. Philip Stark, Pls. Ex. E to Defs. Mot. Exclude Patrick, ECF No. 424-5.

Plaintiffs' argument to exclude Mr. Cotton is inherently flawed. The same grounds that Plaintiffs' motion asserts to exclude Ben Cotton would necessarily exclude the opinions of Plaintiffs' academic cybersecurity expert. For example, Plaintiffs' expert has never worked at a Secretary of State's Office that oversees elections. He has never worked in the electronic voting industry. He has never managed an election utilizing an electronic voting system. Plaintiff's expert is not an election auditor and has never been employed to conduct audits. The "experience" that Plaintiffs' expert has is primarily academia and research. He does not believe a forensic examination is necessary and that does not appear to be within his specific area of expertise.

Plaintiffs' expert also relies upon, without any examination, the conclusions drawn by government authorities that post-election audits confirmed the integrity and results of the 2020 election. He was apparently unaware, for instance, that the inventor of the risk limiting audit incorporated into the laws of several states and countries, Dr. Philip Stark, opined as an expert in the *Curling* case, that the state of Georgia's claim to have conducted a risk limiting audit was nothing more than "security theater" and that Georgians should not have confidence that their votes were counted properly much less counted at all. Decl. Philip Stark, Pls. Ex. E to Defs. Mot. Exclude Patrick, ECF No. 424-5.

Dr. Sherman was either unaware *or chose not to mention* in his September 2023 expert report that the Cybersecurity and Infrastructure Security Agency (CISA), the federal agency in charge of election security, was itself being hacked prior to and during the November 2020 election.[1] Nevertheless, Sherman chose to rely on CISA's conclusion that all was well without any

[1] https://www.cisa.gov/news-events/alerts/2020/12/13/active-exploitation-solarwinds-software. This hack occurred just as CISA's director Christopher Krebs was alleging the 2020 was "secure"—a basis on which Plaintiffs rely in raising their arguments in this matter.

examination nor any supporting or investigatory grounds to support should assertions. So it cannot be that a *forensic* examination would be "useless"—certainly not one similar to what Ben Cotton conducted for the U.S. Office of Personnel Management that discovered the largest breach in U.S. history. *See* Cotton Rpt.

Sherman has never *forensically* examined any Smartmatic voting machine that was *actually* used in any U.S. election or *even looked inside of one that was actually used.* Sherman Rpt. at p. 9. Plaintiffs attempt to sidestep this forensic problem by claiming their expert "used" a *similar* machine to the one used in L.A. County—not the exact machines. But even still, Sherman did nothing more than conduct a visual examination of the exterior of the exemplar. He never actually examined inside of the exemplar and offered a rambling caveat in a footnote for why he felt it was unnecessary—later conceding that an internal forensic examination would be helpful. *Id*.

Indeed, a true forensic examination is required to assess whether there was an intrusion into a system—not an academic, external "walkaround" by viewing the physical box that Plaintiffs' try to proffer. This is not surprising—Smartmatic does not believe in transparency though it puts forward its CEO's declaration that the inside of their voting machines are secure. *See* Pls. Mot. Partial Summ. Judg., Ex. 2, Decl. Mugica. Plaintiffs refused to allow Mr. Cotton to conduct a forensic examination of even the similar "exemplar" model, but instead offered only to allow Cotton to conduct a "walkaround" to view the outside of a different machine. *See* Decl. Kacherouff Opp to Pls. Mot. Exclude Cotton. For forensic purposes, Mr. Cotton opines that merely walking around a computer box is a useless exercise. *See* Decl. Cotton. More is needed to comply

with accepted cybersecurity industry standards for a forensic examination. *Id.* But this is the tactic Plaintiffs have chosen in this case and they are stuck with it.[2] *See* Decl Kacheroff.

Plaintiffs certainly cannot argue the exclusion of Mr. Cotton while introducing Dr. Sherman under the same standards they claim Mr. Cotton is disqualified. Both Mr. Cotton and Plaintiffs' expert Dr. Sherman are cybersecurity experts with opposing opinions that would permit the necessary context for the finder of fact to determine vulnerabilities in electronic voting systems at issue in this case. It is noteworthy that the finder of fact, at a minimum, hear Mr. Cotton's opposing view that a forensic examination consisting internal component examinations and software analysis be measured against the opinion of Plaintiffs' Dr. Sherman—who believes looking at the outside of machines is sufficient to assess internal vulnerabilities. This is especially poignant given the fact that L.A. County's system suffered a breach during the November 2020 election when it was discovered that sensitive voter data and election worker data was found residing on telecom servers of the Chinese Communist Party. See *October 4, 2022: Head of Election Worker Management Company Arrested in Connection with Theft of Personal Data,* Los Angeles County District Attorney's Office, *available at* https://da.lacounty.gov/media/news/head-election-worker-management-company-arrested-connection-theft-personal-data. Smartmatic's work was networked to that L.A. County system alongside Konnech's system.

[2] Of particular note, Plaintiffs' expert agrees with Cotton because he admits that one cannot know whether there was an intrusion by noting potential security weaknesses or citing the existence of technical flaws. PLT Sherman Rebuttal Rpt. at 4. Yet rather than admit a forensic examination is necessary, Plaintiffs' expert chooses to rely on audit reports made by the very same state agencies who are running the elections. Id. at 5.

LEGAL STANDARD

Federal Rule of Evidence 702 and the principles set forth in *Daubert v. Merrell Dow Pharmaceuticals, Inc.,* 509 U.S. 579 (1993) govern this Court's gatekeeping function to ensure the "liberal admission of expert testimony." *Johnson v. Mead Johnson & Co.*, 754 F.3d 557, 562 (8th Cir. 2014); *see, e.g., United States v. Finch,* 630 F.3d 1057, 1062 (8th Cir.2011) (doubts about the usefulness of expert testimony resolved in favor of admissibility); *Robinson v. GEICO Gen. Ins. Co.,* 447 F.3d 1096, 1100 (8th Cir.2006) (expert testimony should be admitted if it "advances the trier of fact's understanding to any degree"); *Lauzon v. Senco Prods., Inc.,* 270 F.3d 681, 686 (8th Cir.2001) (Rule 702 "clearly is one of admissibility rather than exclusion"); *Wood v. Minn. Mining & Mfg. Co.,* 112 F.3d 306, 309 (8th Cir.1997) (holding that exclusion of expert's opinion is proper "only if it is so fundamentally unsupported that it can offer no assistance to the jury").

The Eighth Circuit requires that the proponent of expert testimony establish admissibility by a preponderance of the evidence. *In re Bair Hugger Forced Air Warming Devices Products Liability Litigation*, 9 F.4th 768, 776 (8th Cir. 2021).

While it applied the preponderance standard, *Bair Hugger* court also recognized that the *Daubert* decision expressly calls for the liberal admission of expert testimony. *In re Bair Hugger*, 9 F.4th at 777. The Eighth Circuit (like many other courts) has repeatedly held that "the factual basis of an expert opinion goes to the credibility of the testimony, not its admissibility." *Id.* at 778. The Eighth Circuit has also made clear that gaps in the expert's knowledge generally go to credibility as well, and do not inevitably require exclusion of the expert's opinion. *See e.g., Robinson v. GEICO Gen. Ins*., 447 F.3d 1096, 1100 (8th Cir. 2006).

Courts within the Eighth Circuit have consistently ruled that an expert's general expertise in a relevant field can qualify them to testify on specific issues, provided they rely on a reliable methodology. *Wheeling Pittsburgh Steel Corp. v. Beelman River Terminals, Inc*., 254 F.3d 706, 715 (8th Cir. 2001).

The *Blair Hugger* opinion boiled down Rule 702's screening requirement into a three-part test:

> First, the testimony must be useful to the finder of fact in deciding the ultimate issue of fact, meaning it must be relevant. Second, the expert must be qualified to assist the finder of fact. Third, the testimony must be reliable or trustworthy in an evidentiary sense. . . . 'The standard for judging the evidentiary reliability of expert evidence is 'lower than the merits standard of correctness.'

In re Bair Hugger, 9 F.4th 768, 777 (8th Cir. 2021) (citations omitted). Benjamin Cotton's expert report and testimony satisfies all these criteria.

ARGUMENT AND AUTHORITIES

I. Benjamin Cotton is a highly qualified expert in the field of forensic cybersecurity examinations.

A. Benjamin Cotton has the requisite educational background and extensive years of experience sufficient to provide opinion, testimony, and analysis in this matter.

Under Federal Rule of Evidence 702, expertise may be demonstrated through knowledge, skill, experience, training, or education. In addition, the Eighth Circuit has emphasized a flexible approach to determining expert qualifications, allowing for practical experience to meet the standard. *Robinson v. GEICO Gen. Ins. Co*., 447 F.3d 1096, 1101 (8th Cir. 2006). Mr. Cotton has both the requisite education and experience in cybersecurity including forensic investigations.

Ben Cotton obtained a master's degree in information technology management from the University of Maryland and has numerous technical certifications. *See* Cotton Rpt., Pls. Ex. A,

ECF No. 416-2; *see also* Decl. Cotton. For example, he holds accreditation as a Certified Information Systems Security Professional (CISSP) approved by the U.S. Department of Defense. *Id.* Before one can sit for the extensive CISSP exam, a candidate is required to have a minimum of five years of direct, full-time experience in at least two of eight specialized domains: Security and risk management, Asset security, Security architecture and engineering, Communication and network security, Identity and access management, Security assessment and testing, Security operations, and Software development security. *Id.*

Mr. Cotton also holds accreditation as a Microsoft Certified Professional (MCP), he holds a Network+ certification, and he is a Certified CyFIR Forensics and Incident Response Examiner. *Id.* A certified cyber forensics and incident response examiner is a professional who has earned a certification demonstrating expertise in both digital forensics, which involves collecting and analyzing digital evidence from computers and devices, and incident response, which focuses on identifying, containing, and mitigating cyber security breaches.

Mr. Cotton's practical experience in the workforce consists of over twenty-six (26) years in conducting and performing computer forensics and digital systems analysis. *Id.* He has been an instructor of computer forensics and incident response and has taught students in the EnCase Endpoint Investigator, a digital investigation software tool from Guidance Software that allows investigators to remotely access and search devices like laptops, desktops, and servers. This tool is designed to help investigators collect and preserve evidence in a forensically sound way, making it admissible in court.

Indeed, Mr. Cotton has testified as an expert witness in state and federal courts and before the United States Congress. *Id.* As he notes in his report, he regularly leads engagements involving

digital forensics and cyber security investigations. Cotton Rpt., at p. 2. He has also *forensically* examined voting systems in several states and counties. *See* Cotton Rpt. He has thoroughly examined user manuals of the major voting systems, including Los Angeles County's VSAP system. *Id.* Unfortunately, Smartmatic refused to allow a forensic examination of any system relating the VSAP system. Rather, they presented a self-serving declaration from their own CEO claiming the VSAP source code contained no malware and that the machines were not connected to the internet—without ever allowing Lindell to conduct a forensic investigation. *See* Pls. Mem. Supp. Summ. Judg., Decl. Mugica, Ex. 2.

So, it is abundantly clear that Mr. Cotton's report (filed on September 22, 2023) shows extensive experience in cybersecurity, network forensics, and analysis of election systems across jurisdictions. *See* Cotton Rpt., Pls. Ex. A. Mr. Cotton's education and experience directly relates to identifying systemic vulnerabilities in voting systems, including the VSAP system that Smartmatic played a role in developing. *Id.*

B. Plaintiffs' frivolous argument that Benjamin Cotton requires a "formal education in Voting Systems Technology" fails because such formal education or degree does not exist, and in any event, is not required for an expert opinion.

There is no specialized educational degree that exists for "voting systems" despite Plaintiffs argument that such be required to provide analysis in this matter. Mr. Cotton has formal and extensive education in information technology and extensive experience in examination of voting systems—a far more prestigious educational and experience background than Plaintiffs' expert Dr. Sherman has. Sherman has no formal education in any voting machine systems. Federal Rule of Evidence 702 permits experts to testify based on specialized experience. Mr. Cotton's professional background in identifying security weaknesses translates effectively to assessing

election technology which is itself a computerized system consisting of *multiple* components, machinery, and networking with the Counties and precincts they operate in.

As an example, in 2015, Mr. Cotton personally wrote and developed malware detection software, and then he conducted a demonstration of that software for the U.S. Office of Personnel Management. Decl. Cotton. In so doing, he discovered the largest breach of a U.S. Government network, one that had been ongoing for three years.[3] And this, even though OPM believed its systems were already secure. The confidential information of 4.2 million federal employees were compromised by China. *See* Decl. Cotton.

II. Mr. Cotton's opinions are useful and helpful to the jury in deciding the ultimate issues of fact in this case.

The basis for Mr. Cotton's opinions includes an extensive review of documentation produced by L.A. County concerning its VSAP system. *See* Cotton Rpt., Pls. Ex. A; Decl. Cotton. Mr. Cotton's conclusions derive from an analysis of patterns and vulnerabilities he has personally observed in multiple voting systems, including those manufactured by leading vendors. *Id.* This broader context provides sufficient factual grounding to hypothesize potential issues with the VSAP system.

He can opine on what the log files would show in a computer system such as connected election equipment, whether tampering occurred, whether the system was connected to the internet, whether a ballot marking device produces a voter verifiable ballot, and whether the

[3] *How OPM bilked a security contractor,* (Foreign Policy Sept. 7, 2016), *available at* https://foreignpolicy.com/2016/09/07/how-opm-bilked-a-security-contractor-that-confirmed-a-major-hack-cytech/.

system as a whole comports with federal cybersecurity standards. This is helpful to the jury in determining issues such as falsity or the lack of evidence to prove falsity.

Restrictions imposed by Smartmatic prevented Mr. Cotton from performing a direct analysis, leaving him to rely on analogous systems and industry standards, which is far more than Plaintiffs' expert has relief on with his "external" walkaround assessment. *See* Decl. Kacheroff.

CONCLUSION

For the foregoing reasons, Defendants Michael Lindell and My Pillow respectfully request this Court deny Plaintiffs' motions to exclude expert report and testimony of Benjamin Cotton.

Dated: December 13, 2024.

Respectfully Submitted,

MCSWEENEY, CYNKAR & KACHOUROFF, PLLC

By */s/ Christopher I. Kachouroff*
Christopher I. Kachouroff* (Bar No. 44216)
13649 Office Place, Suite 101
Woodbridge, Virginia 22192
Telephone: (703) 621-3300
chris@mck-lawyers.com

Douglas G. Wardlow (MN Bar #339544)
Jeremiah D. Pilon (MN Bar #392825)
1550 Audubon Rd.
Chaska, MN 55318
Telephone: (952) 826-8658
doug@mypillow.com
jpilon@mypillow.com

ATTORNEY FOR MY PILLOW, INC. AND MICHAEL LINDELL

*Admitted *Pro Hac Vice*